⑲日本国特許庁(JP) ⑪特許出願公開

⑫公開特許公報(A) 平3−100753

⑤Int.Cl.[5]		識別記号		庁内整理番号	⑬公開 平成3年(1991)4月25日
G 06 F	15/00	330	E	7218−5B	
	11/00	340		7343−5B	
	12/14	320	D	7737−5B	

審査請求 未請求 請求項の数 1 (全4頁)

⑤発明の名称 個人識別装置の自己破壊方法

⑩特 願 平1−238229
⑫出 願 平1(1989)9月13日

⑦発 明 者 新 崎 卓 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
⑦発 明 者 井 垣 誠 吾 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
⑦出 願 人 富士通株式会社 神奈川県川崎市中原区上小田中1015番地
⑦代 理 人 弁理士 井島 藤治 外1名

明 細 書

1. 発明の名称

個人識別装置の自己破壊方法

2. 特許請求の範囲

個人識別装置に外力が加えられたことを検出すると(ステップ1)、

警報を発生し(ステップ2)、

登録データ、照合回路、制御回路等を破壊手段を用いて破壊する(ステップ3)ようにしたことを特徴とする個人識別装置の自己破壊方法。

3. 発明の詳細な説明

【概要】

指紋照合装置等の個人識別装置の自己破壊方法に関し、

個人識別装置に外力が加えられた時に、登録データ等を確実に破壊して、より高いセキュリティを維持することを目的とし、

個人識別装置に外力が加えられたことを検出すると、警報を発生し、登録データ、照合回路、制御回路等を破壊手段を用いて破壊するように構成する。

【産業上の利用分野】

本発明は指紋照合装置等の個人識別装置の自己破壊方法に関する。

近年、コンピュータが広範な社会システムのなかに導入されるに伴い、システム・セキュリティに関係者の関心が高まっている。コンピュータルームへの入室や、端末利用の際の本人の確認手段として、これまで用いられてきたIDカードやパスワードには、セキュリティ確保の面から多くの疑問が提起されている。これに対し、指紋は万人不同、終生不変という2大特徴をもつため、本人確認の最も有力な手段と考えられている。

このような個人識別方法にはその本人確認の信頼性と共に、外力が加えられたら情報の秘密性を保持するために、個人に関する情報等は破壊することが望ましい。

【従来の技術】

前述した指紋を用いた個人識別装置の場合、予め登録しておいた個人毎の指紋パターンと入力された指紋パターンとを照合し、一致した場合に本人であると判断している。この種の個人識別装置は、重要施設への入出管理等に用いられる。また、鍵のあるところならどこでも適用されうる。

第５図は個人識別装置の一種である指紋照合システムの従来構成例を示すブロック図である。このようなシステムでは、指紋を画像として扱うのが通常である。指紋入力センサ１から読取られた指紋画像信号（アナログ信号）は、続く入力装置２により画像データ（ディジタルデータ）に変換され、照合装置３に送られる。

照合装置３には、予め個人毎の指紋の画像データ（指紋特徴点データ）を記憶した記憶装置４が接続されている。そして、照合装置３は入力されてきた指紋画像データから指紋特徴点データを抽出し、記憶装置４に格納されている登録された指紋特徴点データと照合する。照合の結果、両方の特徴点が一致したら、本人であるとの確認ができたことになる。

〔発明が解決しようとする課題〕

ただし、このような指紋照合システムから指紋特徴点データを記憶した記憶装置４を盗まれた場合、登録者と同じ特徴を備えた指紋のレプリカを作られ、悪用されるおそれがある。その対策として画像データを暗号化する方法もあるが、照合システムそのものが盗難にあい、制御用回路、照合用回路が解析されてしまうと、暗号化した指紋特徴点データでも解析されるおそれがある。また、制御用回路を解析し、制御用回路になんらかの変更を加えることにより、指紋の照合をせずとも重要施設に進入することが可能となる。

本発明はこのような課題に鑑みてなされたものであって、個人識別装置に外力が加えられた時に、登録データ等を確実に破壊して、より高いセキュリティを維持することができる個人識別装置の自己破壊方法を提供することを目的としている。

〔課題を解決するための手段〕

第１図は本発明方法の原理を示すフローチャートである。本発明は、

個人識別装置に外力が加えられたことを検出すると（ステップ１）、

警報を発生し（ステップ２）、

登録データ，照合回路，制御回路等を破壊手段を用いて破壊する（ステップ３）ようにしたことを特徴としている。

〔作用〕

個人識別装置に何らかの外力が作用したことを検出したら、登録データ，照合回路，制御回路等を強制的に破壊するようにする。これにより、個人に関する情報を確実に破壊して高いセキュリティを維持することができる。

〔実施例〕

以下、図面を参照して本発明の実施例を詳細に説明する。

第２図は本発明方法を実施するシステム構成例を示す図である。１０は個人識別装置であり、その内部に光検知器１１を備えている。この光検知器１１は回路破壊装置１２と接続されており、該回路破壊装置１２から外部にオン・オフ信号入力プラグ１３が出ている。

このように構成された装置において、個人識別装置１０の外箱に外力が加えられ、破壊されると、外部より装置内部に外光が進入する。光検知器１１はこの光を検出すると、警報器（図示せず）を作動させ、異常の発生を知らせる。それと同時に、回路破壊装置１２にその旨の信号を与える。回路破壊装置１２は、外光の進入を知ると、メモリのリセットによる登録指紋画像データ（特徴点データ）の消去，制御用回路，照合用回路のＲＯＭデータの消去，または高電圧によるＬＳＩ，ＩＣ等の破壊を行う。なお、オン・オフ信号入力プラグ１３は回路破壊装置１２の作動／非作動の切替えを行うための信号入力部を構成しており、例えば、オン信号をオン・オフ信号入力プラグ１３より入

力した場合は、回路破壊装置１２は作動待機状態となる。また、オフ信号をオン・オフ信号入力プラグ１３より入力した場合は、回路破壊装置１２は作動停止状態となる。

第３図は本発明方法を実施する他のシステム構成例を示す図で、センサに磁気検知器を用いたものである。図において、２０は個人識別装置で錠２１に取付けられている。２０ａは個人識別装置２０内に設けられている照合装置、記憶装置等の回路（以下内部回路という）である。

２２は個人識別装置２０内に設けられた磁気検知器で回路破壊装置２３と接続されている。２４はオン・オフ信号入力プラグで、その機能は第２図のそれと同一である。２５は磁気検知器２２と対応する位置に設けられた磁石で、扉２１の内側又は室内に取付けられている。２６は磁気検知器２２と接続された警報器である。

このように構成されたシステムにおいて、所定の手順を踏まずに個人識別装置２０が扉２１面より強制的に剥がされた場合には、磁気検知器２２が磁石２５より遠ざかるため、その出力が弱くなる。これにより、磁気検知器２２は個人識別装置２０が扉面から剥がされたことを検出することができる。これにより、磁気検知器２２は異常の発生を検出し、警報器２６を作動させて異常を報告する。それと同時に、回路破壊装置２３に異常を通知する。回路破壊装置２３は異常通知を受けると、内部回路２０ａを破壊する。これにより、個人に関する情報が盗難されるという不測の事故の発生を予防することができる。

第４図は本発明方法を実施する他のシステム構成例を示す図であり、センサとして振動検知器を用いたものである。図において、３０は個人識別装置で、その内部に第３図と同様の内部回路３０ａが内蔵されている。３１は振動を検出してその解析も行う振動検知器、３２は該振動検知器３１の出力を受けて回路破壊動作を行う回路破壊装置である。３３は振動検知器３１と接続された警報器である。３４は第３図に示すそれと同様の構造を持つオン・オフ信号入力プラグである。

このように構成されたシステムにおいて、振動検知器３１が外箱の破壊や取外しの時に発生する振動を検出すると、警報器３３を動作させて異常の発生を報告すると共に、回路破壊装置３２にその旨を通知する。これにより、回路破壊装置３２は内部回路３０ａを破壊する。具体的には、メモリのリセットによる画像データの消去、制御用回路，照合用回路のＲＯＭデータの消去又は高電圧によるＬＳＩ，ＩＣ等の破壊を行う。なお、この場合において、異常による振動と地震による振動とは地震による振動が持つＰ波，Ｓ波を検出することで識別ができる。

なお、上述した全ての実施例において、一連の動作はバックアップ電源（例えば電池等）により行い、個人識別装置の電源が切断された場合でも作動するように構成しておく必要がある。また、上述したシステムを工場で生産したり、設置後のメインテナンスを行うためには、破壊装置を自由に作動，停止させる機能が必要になる。破壊装置の動作開始をするための方法として、破壊装置の動作を停止させるためには、個人識別装置外箱に設けられた信号入力プラグから停止信号を入力する方法や、個人識別装置外箱に設けられた穴より工具を用いて動作停止信号を入力する方法等が用いられる。なお、オン・オフ信号入力プラグに許容値以上の電流又は電圧が印加された場合には、即座に破壊装置が動作を開始するようにしておく。

〔発明の効果〕

以上、詳細に説明したように、本発明によれば個人識別装置に外力（破壊，衝撃，開封等）が加わった時に、そのことを検出して装置内の登録データ，制御用回路，照合回路等を全て又は一部破壊することにより、登録データの盗難、悪用を防ぐことができ、更に制御系，照合系の解析を不可能とすることができ、実用上の効果が大きい。

4．図面の簡単な説明

第１図は本発明方法の原理を示すフローチャート、

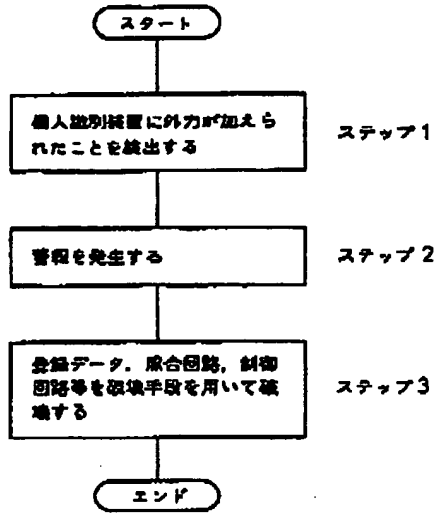
第２図は本発明方法を実施するシステム構成例

を示す図、

第3図，第4図は本発明方法を実施する他のシステム構成例を示す図、

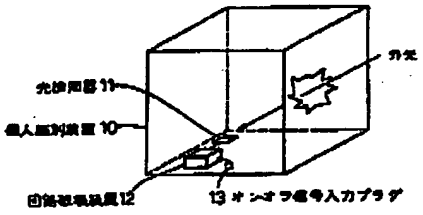
第5図は指紋照合システムの従来構成例を示すブロック図である。

特許出願人　富士通株式会社
代理人　弁理士　井桁貞一
外1名



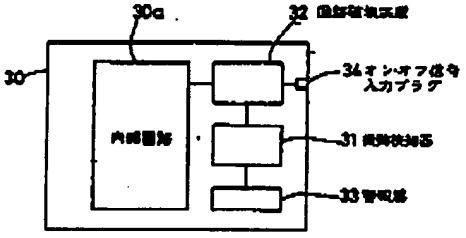
本発明方法の原理を示すフローチャート

第 1 図



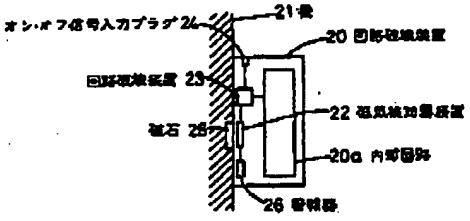
本発明方法を実施するシステム構成例を示す図

第 2 図



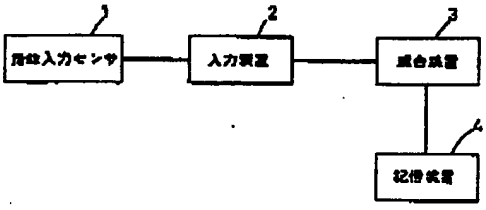
本発明方法を実施する他のシステム構成例を示す図

第 4 図



本発明を実施する他のシステム構成例を示す図

第 3 図



指紋照合システムの従来構成例を示すブロック図

第 5 図

English-Language Translation of JP 3-100753

(19) Japanese Patent Office (JP)

(12) Publication of Unexamined Patent Applications (A)

(11) Patent Application Publication No. Hei 3-100753

(43) Date of Publication: April 25, 1991

(51) Int.Cl.[5]

Domestic Classification Symbol

Internal Reference No.

(54) Title of the Invention: Examination requested or not: Not requested; No. of Claims: 1 (4 pages in total)

Self-Destroying Method for Personal Identification Apparatuses

(21) Application No.: Patent Application Hei 1-238229

(22) Date of Application: September 13, 1989

(72) Inventor: Takashi Arasaki, c/o FUJITSU LIMITED, 1015, Kamikodanaka, Nakahara-ku, Kawasaki-shi, Kanagawa-ken

(72) Inventor: Seigo Igaki, c/o FUJITSU LIMITED, 1015, Kamikodanaka, Nakahara-ku, Kawasaki-shi, Kanagawa-ken

(71) Applicant: FUJITSU LIMITED, 1015, Kamikodanaka, Nakahara-ku, Kawasaki-shi, Kanagawa-ken

(74) Representatives: Toji Ijima, patent attorney, and one other person

SPECIFICATION

1. Title of the Invention

Self-Destroying Method for Personal Identification Apparatuses

2. Scope of the Claims

A self-destroying method for personal identification apparatuses, characterized in that:

upon detection of an external force applied to a personal identification apparatus (step 1),

an alarm is issued (step 2), and

registered data, collating circuits, control circuits and the like are destroyed by using destroying means (step 3).

3. Detailed Description of the Invention

[Summary]

The invention relates to a self-destroying method for personal identification apparatuses, such as fingerprint collation apparatuses or the like,

is intended to maintain a higher level of security by reliably destroying registered data and the like when an external force is applied to a personal identification apparatus, and

is so configured as to issue an alarm upon detecting the application of an external force on the personal identification apparatus, and to destroy registered data, collating circuits, control circuits and the like by using destroying means.

[Field of Industrial Application]

The present invention relates to a self-destroying method for personal identification apparatuses, such as fingerprint collation apparatuses or the like.

In recent years, along with the introduction of computers in extensive social systems, interested parties' concern is focusing on system security. Many questions have been raised with a view to ensuring security to ID cards and passwords conventionally used as personal identification means for entrance into a computer room or using a terminal. In this connection, fingerprints are considered the most useful means for personal identification on account of their two major characteristics including the difference from individual to individual without exception and the unchangeability for life.

For such a method of personal identification, it is desirable to enable information on individuals and the like to be destroyed to secure the confidentiality of information to which an external force has been applied in addition to ensuring credibility of personal identification.

[Prior Art]

In the case of the aforementioned personal identification apparatus, an inputted fingerprint pattern is collated with the personal fingerprint pattern registered in advance and, when they are found identical, the former is judged to be

legitimate. This kind of personal identification apparatus is used for managing entrances to and exits from important facilities among other purposes. It also can be applied anywhere as long as there is a lock.

Fig. 5 is a block diagram showing an example of conventional configuration of a fingerprint collating system, which is a kind of personal identification apparatus. In such a system, a fingerprint is usually handled as an image. A finger print image signal (analog signal) inputted from a finger print input sensor 1 is converted into image data (digital data) by an input device 2 that follows, and delivered to a collating device 3.

To the collating device 3 is connected a memory device 4 in which image data of person-by-person fingerprints (fingerprint characteristic point data) is stored in advance. And the collating device 3 extracts fingerprint characteristic point data from the inputted fingerprint image data, and collates it with registered fingerprint characteristic point data stored in the memory device 4. If as a result of collation the characteristic points of both are found identical, the person will be identified as such.

[Problems to be Solved by the Invention]

If the memory device 4 storing fingerprint characteristic point data is stolen from such a fingerprint collating system, replicas of fingerprints having the same characteristics as registrants may be made and abused.

Precautionary measures include a method of enciphering the image data, but if the collating system is stolen and its control circuits and collating circuits are analyzed, even the enciphered fingerprint characteristic point data may be analyzed. Further, by analyzing the control circuits and making some alteration in the control circuits, entrance into the important facility without having to go through fingerprint collation may be made possible.

The present invention, attempted in view of these problems, is intended to provide a self-destroying method for personal identification apparatuses enabling, when an external force is applied to a personal identification apparatus, registered data and the like to be reliably destroyed thereby to maintain a higher level of security.

[Means to Solve the Problems]

Fig. 1 is a flowchart illustrating the principle of the method of the present invention. The invention is characterized in that:

upon detection of an external force applied to a personal identification apparatus (step 1),

an alarm is issued (step 2), and

registered data, collating circuits, control circuits and the like are destroyed by using destroying means (step 3).

[Actions]

Upon detection of any external force applied to a

personal identification apparatus, registered data, collating circuits, control circuits and the like are forcibly destroyed by using destroying means. Information regarding individuals can be thereby reliably destroyed to maintain a high level of security.

[Embodiments]

Embodiments of the present invention will be described in detail below with reference to drawings.

Fig. 2 is a diagram showing an example of configuration of the system for implementing the method of the invention. Reference numeral 10 denotes a personal identification apparatus, provided inside with an optical detector 11. This optical detector 11 is connected to a circuit destroying device 12, and an on/off signal input plug 13 extends outward from the circuit destroying device 12.

If, in an apparatus configured in this manner, an external force is applied to the outer case of the personal identification apparatus 10, which is thereby destroyed, an external light comes into the device from outside. Upon detection of this light, the optical detector 11 actuates an alarm (not shown) to make the occurrence of abnormality known. At the same time it gives a signal to that effect to the circuit device destroying device 12. When informed of the entrance of the external light, the device destroying device 12 performs deletion of registered fingerprint image data (characteristic point data) by resetting memories, deletion of ROM data in control circuits and collating

circuits, or destruction of LSIs, ICs and the like with a high voltage. Incidentally, the on/off signal input plug 13 constitutes a signal input unit for switching-over between the operation and non-operation of the device destroying device 12; if, for instance, an on signal is inputted from the on/off signal input plug 13, the device destroying device 12 will be placed in a standby-for-operation state. Or if an off signal is inputted from the on/off signal input plug 13, the device destroying device 12 will be placed in an operation-stopped state.

Fig. 3 is a diagram showing another example of configuration of the system for implementing the method of the invention, wherein a magnetic detector is used as the sensor. In the drawing, reference numeral 20 denotes a personal identification apparatus, which is fitted to a wall 21. Numeral 20a denotes circuits such as a collation device, a memory device and so forth provided within the personal identification apparatus 20 (hereinafter referred to as internal circuits).

Numeral 22 denotes a magnetic detector provided in the personal identification apparatus 20, and the detector is connected to a circuit destroying device 23. Numeral 24 denotes an on/off signal input plug, whose function is the same as that of its counterpart in Fig. 2. Numeral 25 denotes a magnet disposed in a position corresponding to the magnetic detector 22, and the magnet is fitted within or to the surface of the wall 21. Numeral 26 denotes an alarm connected to

the magnetic detector 22.

In the system configured in this manner, if the personal identification apparatus 20 is forcibly peeled off the surface of the wall 21 without a prescribed procedure being gone through, the magnetic detector 22 will move away from the magnet 25 and accordingly its output will weaken. The magnetic detector 22 is thereby enabled to detect the peeling of the personal identification apparatus 20 off the wall surface. This causes the magnetic detector 22 to detect the occurrence of abnormality, and report the abnormality by sounding the alarm 26. At the same time it notifies the circuit destroying device 23 of the abnormality. When notified of the abnormality, the circuit destroying device 23 destroys the internal circuits 20a. A contingent accident of stealing of information on individuals can be thereby prevented from occurring.

Fig. 4 is a diagram showing still another example of configuration of the system for implementing the method of the invention, wherein a vibration detector is used as the sensor. In the drawing, reference numeral 30 denotes a personal identification apparatus, which has, built into it, internal circuits 30a similar to their counterparts in Fig. 3. Numeral 31 denotes a vibration detector which detects vibration and also analyzes it; and 32 denotes a circuit destroying device which, in response to an output of the vibration detector 31, performs a circuit destroying action. Numeral 33 denotes an alarm connected to the vibration

detector 31. Numeral 34 denotes an on/off signal input plug, whose function is the same as that of its counterpart in Fig. 3.

In the system configured in this manner, if the vibration detector 31 detects vibration which would arise when the outer case is destroyed or removed, it will report the abnormality by sounding the alarm 33 and at the same time notify the circuit destroying device 32 of that occurrence. In response, the circuit destroying device 32 destroys the internal circuits 30a. More specifically, it performs deletion of registered fingerprint image data by resetting memories, deletion of ROM data in control circuits and collating circuits, or destruction of LSIs, ICs and the like with a high voltage. Incidentally, in this case vibration due to such abnormality and vibration due to an earthquake can be distinguished from each other by detecting the P wave and the S wave earthquake-deriving vibration would have.

In any of the embodiments described above, the configuration should be such that the sequence of operations be performed with a backup power source (e.g. a battery or the like) so that operation is possible even if the power supply to the personal identification apparatus is cut off. Also, in order to enable the above-described systems to be produced in a factory or to undergo maintenance after their installation, a function to freely actuate and stop the destroying device will be needed. Methods used for actuating the destroying device include, in order to stop the operation

of the destroying device, one by which a stop signal is inputted through a signal input plug disposed on the outer case of the personal identification apparatus and another by which a tool is used to input an operation stop signal through a hole bored in the outer case of the personal identification apparatus. To add, the destroying device is so set as to immediately start operation when a current or a voltage above the permissible limit is applied to the on/off signal input plug.

[Effects of the Invention]

As hitherto described in detail, according to the present invention, it is made possible, when any external force (destruction, robbery, unsealing or the like) is applied to a personal identification apparatus, to detect that occurrence, prevent registered data from being copied or forged by destroying all or some of the registered data, control circuits, collating circuits and the like in the apparatus, and further to make analysis of control and collation lines impossible, resulting in significant practical effects.

4. Brief Description of the Drawings

Fig. 1 is a flowchart illustrating the principle of the method of the present invention;

Fig. 2 is a diagram showing an example of configuration of the system for implementing the method of the invention;

Fig. 3 and Fig. 4 are diagrams showing other examples of configuration of the system for implementing the method

of the invention; and

Fig. 5 is a block diagram showing an example of conventional configuration of a fingerprint collating system.

Applicant for Patent: FUJITSU LIMITED

Representatives: Toji Ijima, patent attorney, and one other person

Fig. 1

Flowchart illustrating principle of invented method

Start

Step 1

Detect application of external force to personal identification apparatus

Step 2

Issue alarm

Step 3

Destroy registered data, collating circuits, control circuits, etc. by using destroying means

End

Fig. 2

Diagram showing example of configuration of system for implementing invented method

External light (外光)

10: Personal identification apparatus

11: Optical detector

12: Circuit destroying device

13: On/off signal input plug

Fig. 3

Diagram showing another example of configuration of system for implementing invented method

20: Personal identification apparatus

20a: Internal circuits

21: Wall

22: Magnetic detector device

23: Circuit destroying device

24: On/off signal input plug

25: Magnet

26: Alarm

Fig. 4

Diagram showing another example of configuration of system for implementing invented method

30a: Internal circuits

31: Vibration detector

32: Circuit destroying device

34: On/off signal input plug

33: Alarm

Fig. 5

Block diagram showing example of conventional configuration of fingerprint collating system

1: Finger print input sensor

2: Input device

3: Collating device

4: Memory device